strongSwan - Feature #740

Support additional PBES2 encryption schemes

17.10.2014 09:26 - Jamil Nimeh

Status:	Closed	**Start date:**	17.10.2014
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libstrongswan		
Target version:	5.2.2		
Resolution:	Fixed		

Description

Not sure whether this is better categorized as a feature or a bug. Maybe more of a feature...

In 5.2.0 and earlier, encrypted PKCS#8 files using PBES2 and any non-3DES algorithm fail to unwrap in Strongswan. It is possible with a small code change to make other algorithms used with PBES2 like DES, RC2, Blowfish and AES accessible in Strongswan. Given openssl's use of PKCS#8 as the default write format for private keys, we may see more keys encrypted with PBES2 and AES. The other older ciphers (DES, RC2, Blowfish) probably won't be found very often, but the changes to enable these ciphers were easy to do once the work for AES was done. I have attached a proof-of-concept fix that will allow Strongswan to unwrap keys generated in this format, for example:

openssl genrsa 2048 | openssl pkcs8 -topk8 -v2 <CIPHER> -out some-p8-enc-key.pem
Where <CIPHER> can be des, des3, aes128, aes192, aes256, bf-cbc, rc2-40-cbc, rc2-64-cbc, or rc2-cbc (128-bit)

The blowfish support requires --enable-blowfish to be added at configure time.

This was tested using Strongswan 5.2.0 on CentOS 7
CentOS Linux release 7.0.1406 (Core)
Linux abbott 3.10.0-123.8.1.el7.x86_64 #1 SMP Mon Sep 22 19:06:58 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux

Associated revisions

Revision 5743f6df - 05.12.2014 14:35 - Tobias Brunner

asn1: Add OID for Blowfish CBC

The OID (1.3.6.1.4.1.3029.1.2) is technically not correct, the correct
one is (1.3.6.1.4.1.3029.1.1.2). Every other library or tool (like OpenSSL)
uses the incorrect one so we do the same.

References #740.

Revision 7bd55485 - 05.12.2014 14:35 - Tobias Brunner

pkcs5: Add support for PBES2 encryption schemes other than 3DES

This allows using e.g. AES for PKCS#8 and PKCS#12 files.

Some legacy schemes defined in RFC 2898 are not supported (like RC2).

Fixes #740.

History

#1 - 17.10.2014 12:45 - Tobias Brunner

- Tracker changed from Issue to Feature

- Status changed from New to Feedback

- Assignee set to Tobias Brunner

I pushed a couple of commits to the *pbes2-algs* branch. I don't think we really need to provide support for the legacy RC2 algorithm, I added the Blowfish OID though.

The Blowfish OID (1.3.6.1.4.1.3029.1.2) is technically incorrect. The correct OID for Blowfish CBC has a one more 1 in there (1.3.6.1.4.1.3029.1.1.2). I saw that it is used incorrectly like that by several libraries/tools (e.g. OpenSSL and BouncyCastle) so this is probably due to an early typo and everybody has to do this incorrectly now.

#2 - 05.12.2014 14:37 - Tobias Brunner

- Status changed from Feedback to Closed

- Target version set to 5.2.2

- Resolution set to Fixed

Implemented with the referenced commits.

Files

ss-pkcs8.patch	6.75 KB	17.10.2014	Jamil Nimeh